Switch Security Issues

An Introduction

Cabrillo College

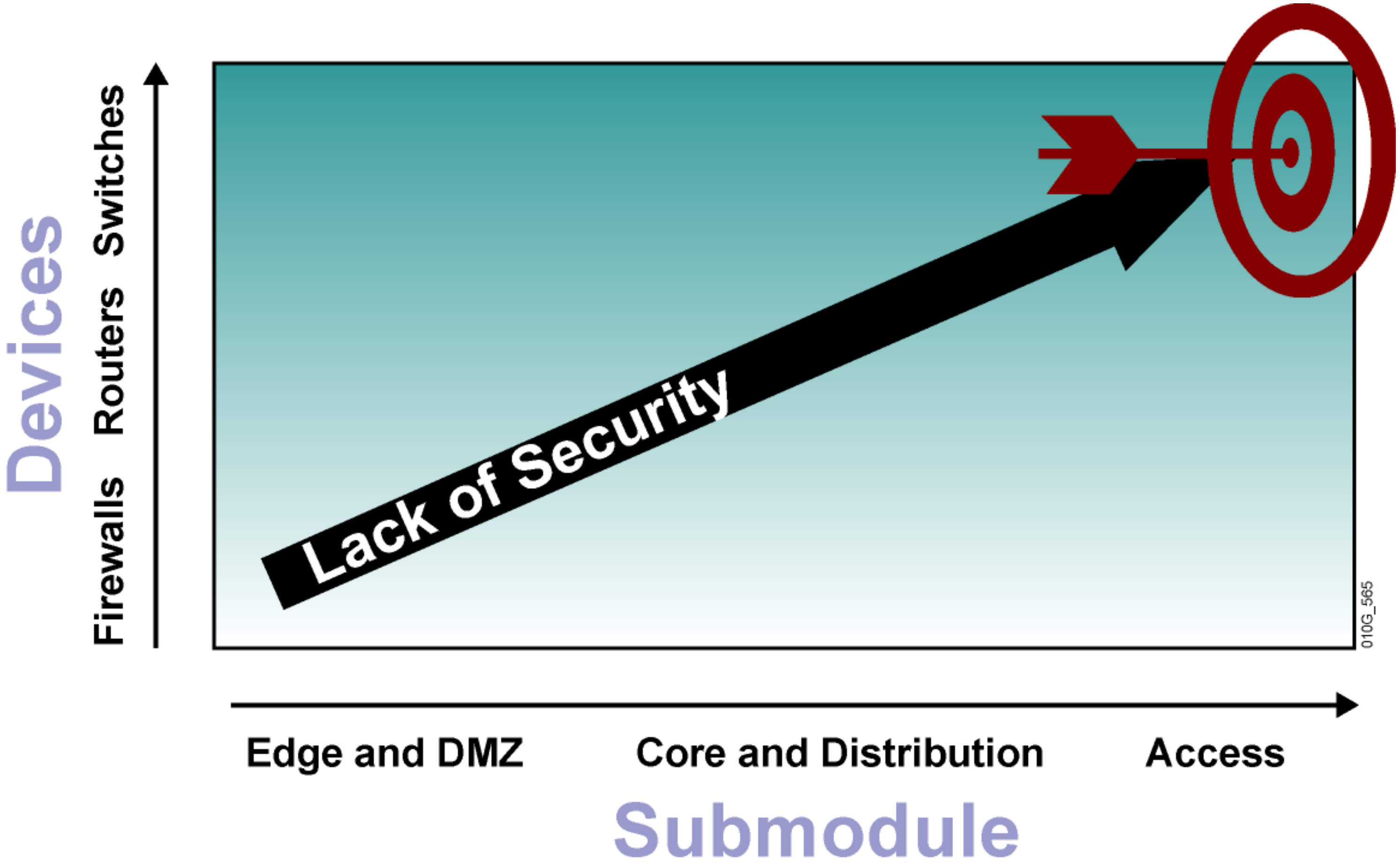
CIS 83 (CCNA 3)

Fall 2006

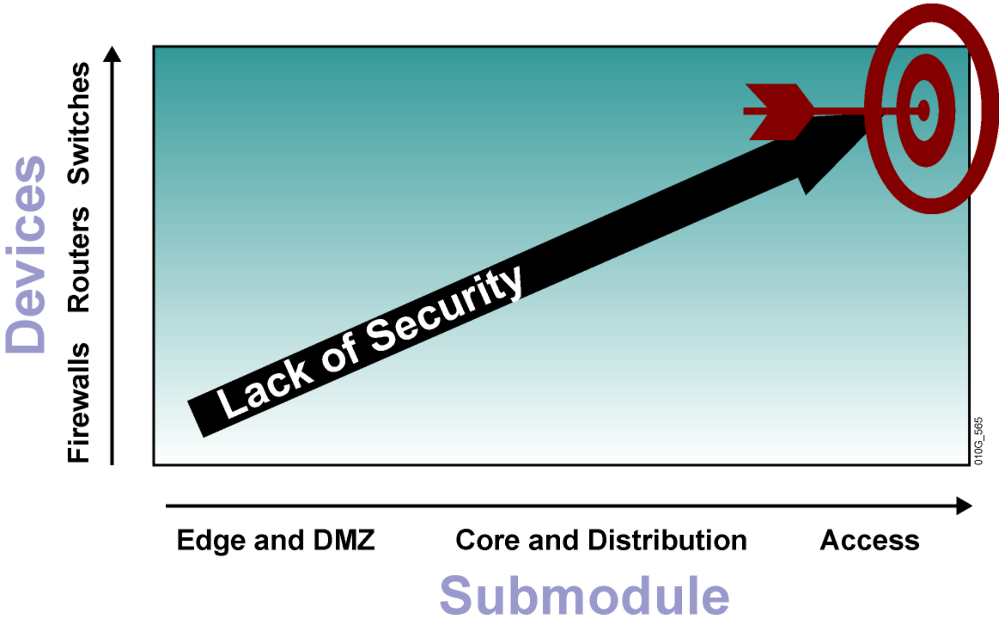
Rick Graziani

Fall 2006

Overview of Switch Security



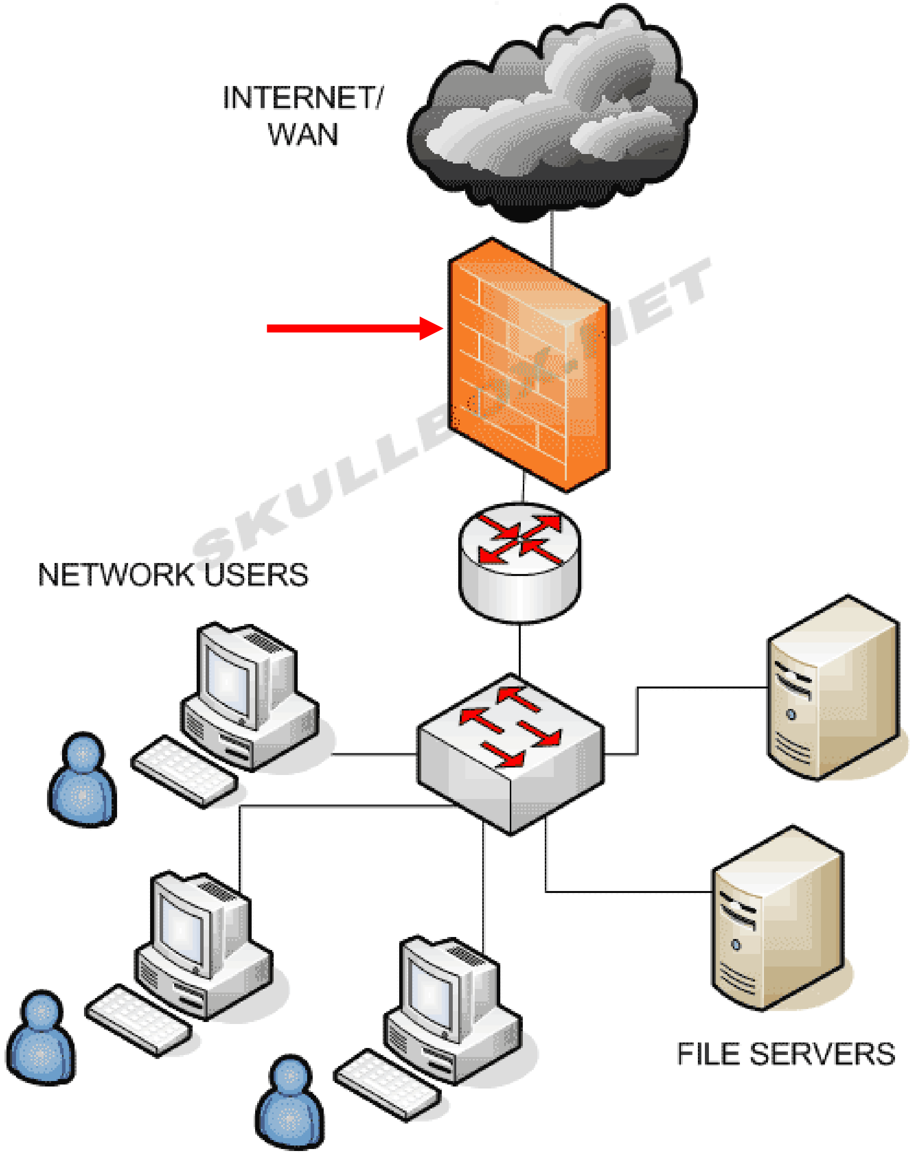
Overview of Switch Security



- Much industry attention surrounds security attacks from outside the walls of an organization.
- Campus access devices and Layer 2 communication are left largely unconsidered in most security discussions.

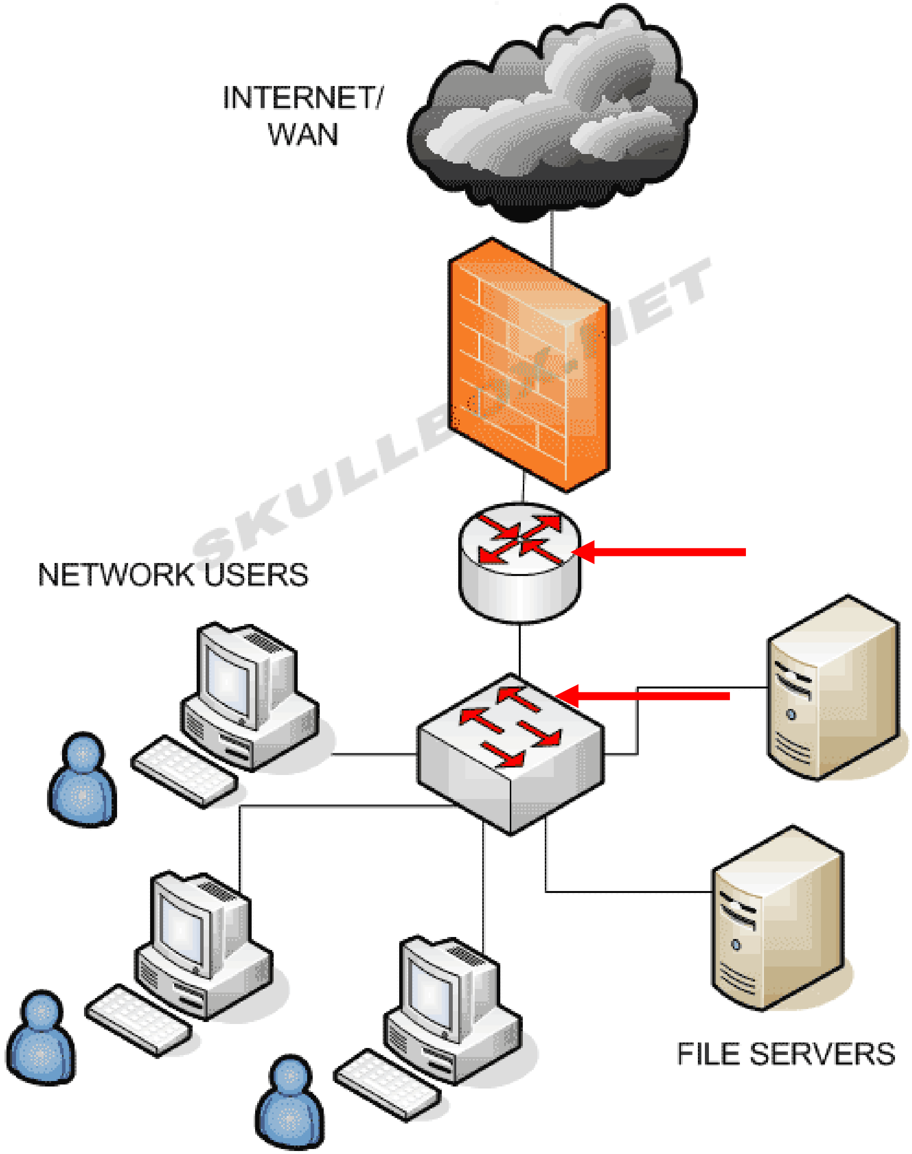
Overview of Switch Security

- The default state of networking equipment:
  - **Firewalls** (placed at the organizational borders)
    - Default: Secure and must be configured for communications.
  - **Routers and switches** (placed internal to an organization)
    - Default: Unsecured, and must be configured for security



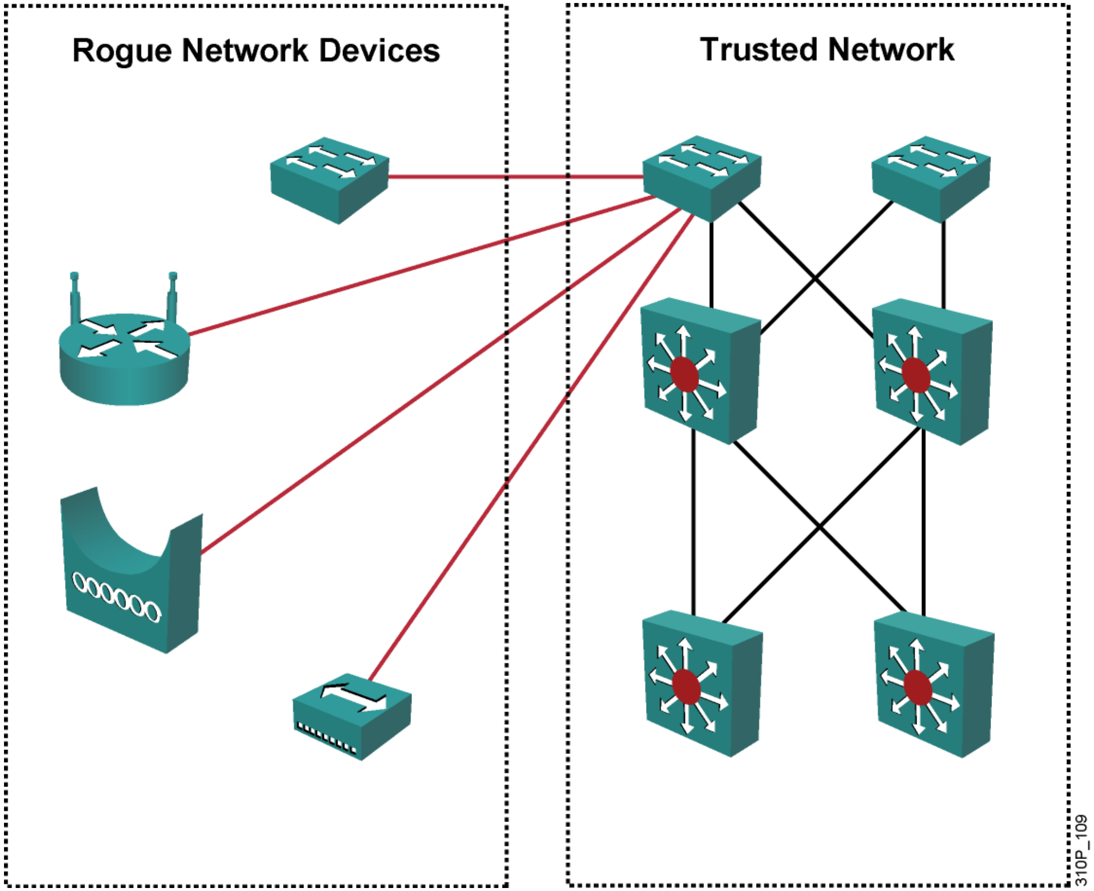
Overview of Switch Security

- If an attack is launched at Layer 2 on an internal campus device, the rest of the network can be quickly compromised, often without detection.
- Due to the increase of malicious activity at Layer 2, security on switches had to be tightened.
- …just like routers.



Rogue Access Points

- Rogue network devices can be:
  - Wireless hubs
  - Wireless routers
  - Access switches
  - Hubs
- These devices are typically connected at access level switches.



Switch Attack Categories

- **MAC layer attacks**
- VLAN attacks
- Spoofing attacks
- Attacks on switch devices

MAC layer attacks

- MAC address flooding
  - Frames with unique, invalid source MAC addresses flood the switch, exhausting content addressable memory (CAM) table space, disallowing new entries from valid hosts.
  - Traffic to valid hosts is subsequently flooded out all ports.
- Solution
  - Port security
  - MAC address VLAN access maps

VLAN attacks (Discussed in CCNP 3)

- VLAN hopping
  - By altering the VLAN ID on packets encapsulated for trunking, an attacking device can send or receive packets on various VLANs, bypassing Layer 3 security measures.
- Solution
  - Tighten up trunk configurations and the negotiation state of unused ports.
  - Place unused ports in a common VLAN.

VLAN attacks (Discussed in CCNP 3)

- Attacks between devices on a common VLAN
  - Devices may need protection from one another, even though they are on a common VLAN.
  - This is especially true on service provider segments supporting devices from multiple customers.
- Solution
  - Private VLANs (PVLANs).

Spoofing attacks (Discussed in CCNP 3)

- DHCP starvation and DHCP spoofing
  - An attacking device can exhaust the address space available to the DHCP servers for a period of time or establish itself as a DHCP server in man-in-the-middle attacks
- Solution
  - DHCP snooping

Spoofing attacks (Discussed in CCNP 3)

- Spanning tree compromises
  - Attacking device spoofs the root bridge in the STP topology.
  - If successful, the network attacker can see a variety of frames.
- Solution
  - Proactively configure the primary and backup root devices.
  - Enable root guard.

Spoofing attacks (Discussed in CCNP 3)

- MAC spoofing
  - Attacking device spoofs the MAC address of a valid host currently in the CAM table.
  - Switch then forwards frames destined for the valid host to the attacking device.
- Solution
  - DHCP snooping
  - Port security

Spoofing attacks (Discussed in CCNP 3)

- Address Resolution Protocol (ARP) spoofing
  - Attacking device crafts ARP replies intended for valid hosts.
  - The attacking device’s MAC address then becomes the destination address found in the Layer 2 frames sent by the valid network device.
- Solution
  - Dynamic ARP Inspection
  - DHCP snooping
  - Port security

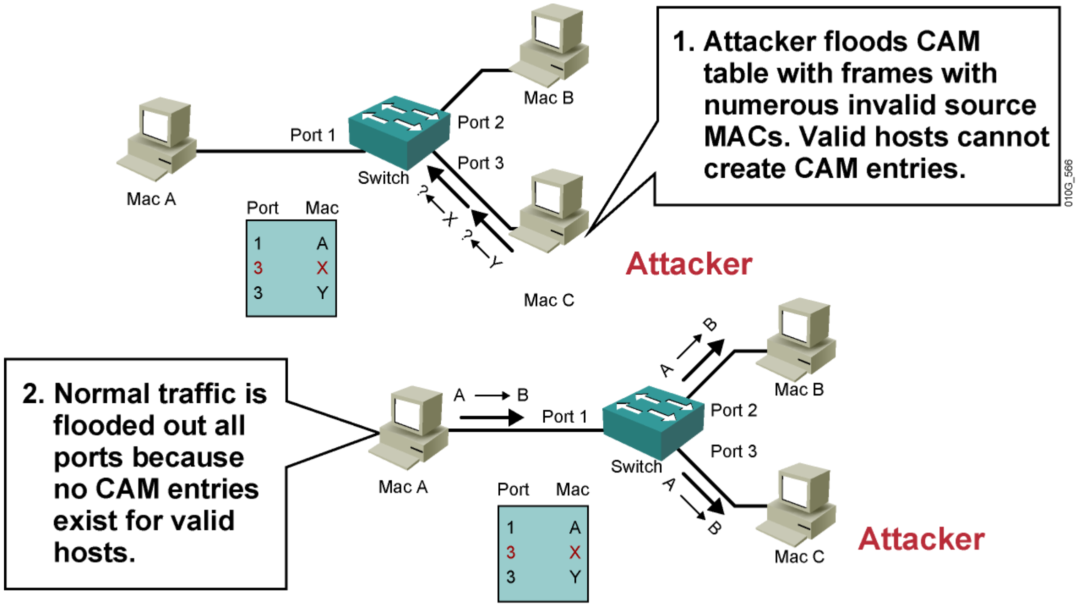
Attacks on switch devices (Discussed in CCNP 3)

- Cisco Discovery Protocol (CDP) manipulation
  - Information sent through CDP is transmitted in clear text and unauthenticated, allowing it to be captured and divulge network topology information.
- Solution
  - Disable CDP on all ports where it is not intentionally used.

Attacks on switch devices (Discussed in CCNP 3)

- Secure Shell Protocol (SSH) and Telnet attacks
  - Telnet packets can be read in clear text.
  - SSH is an option but has security issues in version 1.
- Solution
  - SSH version 2.
  - Telnet with virtual type terminal (VTY) ACLs.

MAC Layer Attacks



1. Attacker floods CAM table with frames with numerous invalid source MACs. Valid hosts cannot create CAM entries.

Port	Mac
1	A
3	X
3	Y

2. Normal traffic is flooded out all ports because no CAM entries exist for valid hosts.

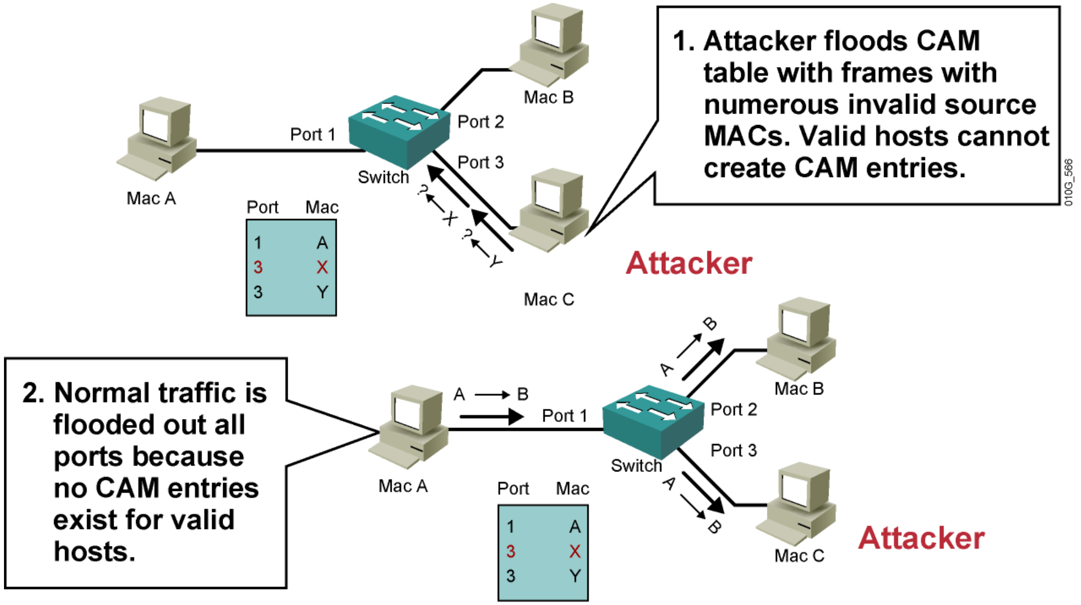
Port	Mac
1	A
3	X
3	Y

- Common Layer 2 or switch attack (“as of this writing”)
- Launched for the malicious purpose of:
  – Collecting a broad sample of traffic

  or

  – Denial of Service (DoS) attack.

MAC Layer Attacks



1. Attacker floods CAM table with frames with numerous invalid source MACs. Valid hosts cannot create CAM entries.

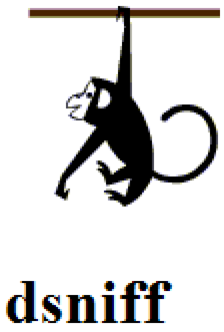
2. Normal traffic is flooded out all ports because no CAM entries exist for valid hosts.

Port	Mac
1	A
3	X
3	Y

Port	Mac
1	A
3	X
3	Y

- Switch’s CAM tables are limited in size (1,024 to over 16,000 entries).
- Tools such as dsniff can flood the CAM table in just over 1 minute.

dniff: http://www.monkey.org/~dugsong/dsniff/



- “dsniff is a collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.).”
- “arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching).”
- “sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.”
- “I wrote these tools with honest intentions - to audit my own network, and to demonstrate the insecurity of most network application protocols. Please do not abuse this software.”

MAC Flooding switches with dsniff

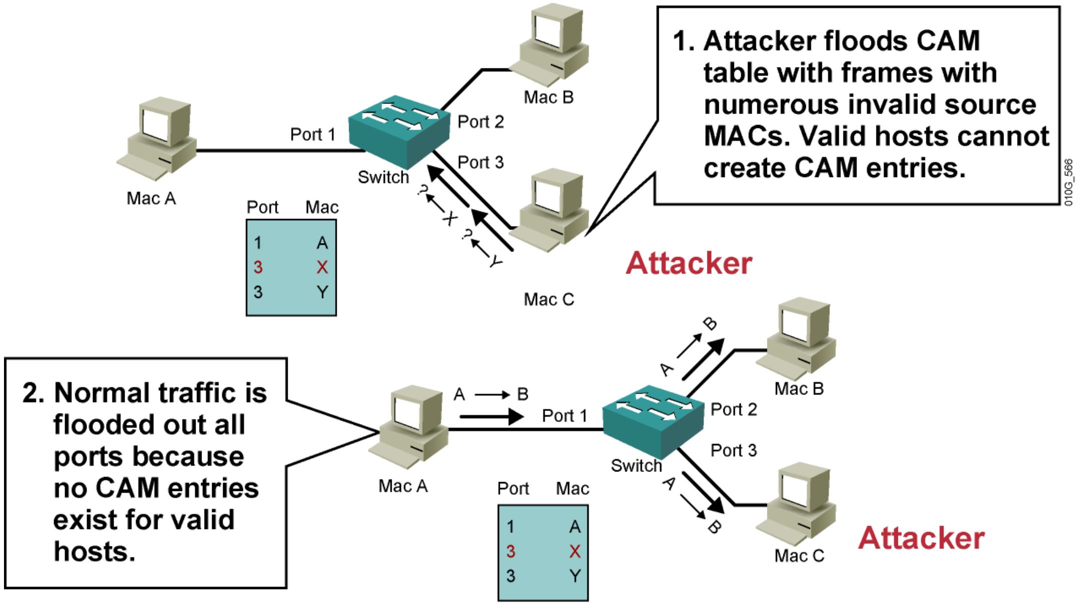
```
[root@sconvery-lnx dsniff-2.3]# ./macof
101.59.29.36 -> 60.171.137.91 TCP D=55934 S=322 Syn Seq=1210303300 Len=0 Win=512
145.123.46.9 -> 57.11.96.103 TCP D=44686 S=42409 Syn Seq=1106243396 Len=0 Win=52
109.40.136.24 -> 51.158.227.98 TCP D=59038 S=21289 Syn Seq=2039821840 Len=0 Win2
126.121.183.80 -> 151.241.231.59 TCP D=7519 S=34044 Syn Seq=310542747 Len=0 Win2
211.28.168.72 -> 91.247.223.23 TCP D=62807 S=53618 Syn Seq=2084851907 Len=0 Win2
183.159.196.56 -> 133.10.138.87 TCP D=23929 S=51034 Syn Seq=1263121444 Len=0 Wi2
19.113.88.77 -> 16.189.146.61 TCP D=1478 S=56820 Syn Seq=609596358 Len=0 Win=512
237.162.172.114 -> 51.32.8.36   TCP D=38433 S=31784 Syn Seq=410116516 Len=0 Win2
 118.34.90.6 -> 61.169.58.50 TCP D=42232 S=31424 Syn Seq=1070019027 Len=0 Win=52
46.205.246.13 -> 72.165.185.7 TCP D=56224 S=34492 Syn Seq=937536798 Len=0 Win=52
105.109.246.116 -> 252.233.209.72 TCP D=23840 S=45783 Syn Seq=1072699351 Len=0 2
60.244.56.84 -> 142.93.179.59 TCP D=3453 S=4112 Syn Seq=1964543236 Len=0 Win=512
151.126.212.86 -> 106.205.161.66 TCP D=12959 S=42911 Syn Seq=1028677526 Len=0 W2
9.121.248.84 -> 199.35.30.115 TCP D=33377 S=31735 Syn Seq=1395858847 Len=0 Win=2
226.216.132.20 -> 189.89.89.110 TCP D=26975 S=57485 Syn Seq=1783586857 Len=0 Wi2
124.54.134.104 -> 235.83.143.109 TCP D=23135 S=55908 Syn Seq=852982595 Len=0 Wi2
 27.54.72.62 -> 207.73.65.108 TCP D=54512 S=25534 Syn Seq=1571701185 Len=0 Win=2
246.109.199.72 -> 1.131.122.89 TCP D=61311 S=43891 Syn Seq=1443011876 Len=0 Win2
 251.49.6.89 -> 18.168.34.97 TCP D=25959 S=956 Syn Seq=6153014 Len=0 Win=512
51.105.154.55 -> 225.89.20.119 TCP D=33931 S=1893 Syn Seq=116924142 Len=0 Win=52
82.2.236.125 -> 210.40.246.122 TCP D=43954 S=49355 Syn Seq=1263650806 Len=0 Win2
21.221.14.15 -> 9.240.58.59  TCP D=61408 S=26921 Syn Seq=464123137 Len=0 Win=512
70.63.102.43 -> 69.88.108.26 TCP D=61968 S=53055 Syn Seq=682544782 Len=0 Win=512
```

MAC Flooding switches with dsniff

- Dsniff (macof) can generate 155,000 MAC entries on a switch per minute
- It takes about 70 seconds to fill the cam table
- Once table is full, traffic without a CAM entry floods on the VLAN.

```
CAT6506 (enable) show cam count dynamic
Total Matching CAM Entries = 131052
```

MAC Flooding



1. Attacker floods CAM table with frames with numerous invalid source MACs. Valid hosts cannot create CAM entries.

Port	Mac
1	A
3	X
3	Y

2. Normal traffic is flooded out all ports because no CAM entries exist for valid hosts.

Port	Mac
1	A
3	X
3	Y

- Once the CAM table is full, new valid entries will not be accepted.
- Switch must flood frames to that address out all ports.
- This has two adverse effects:
  - The switch traffic forwarding is inefficient and voluminous.
  - An intruding device can be connected to any switch port and capture traffic not normally seen on that port.

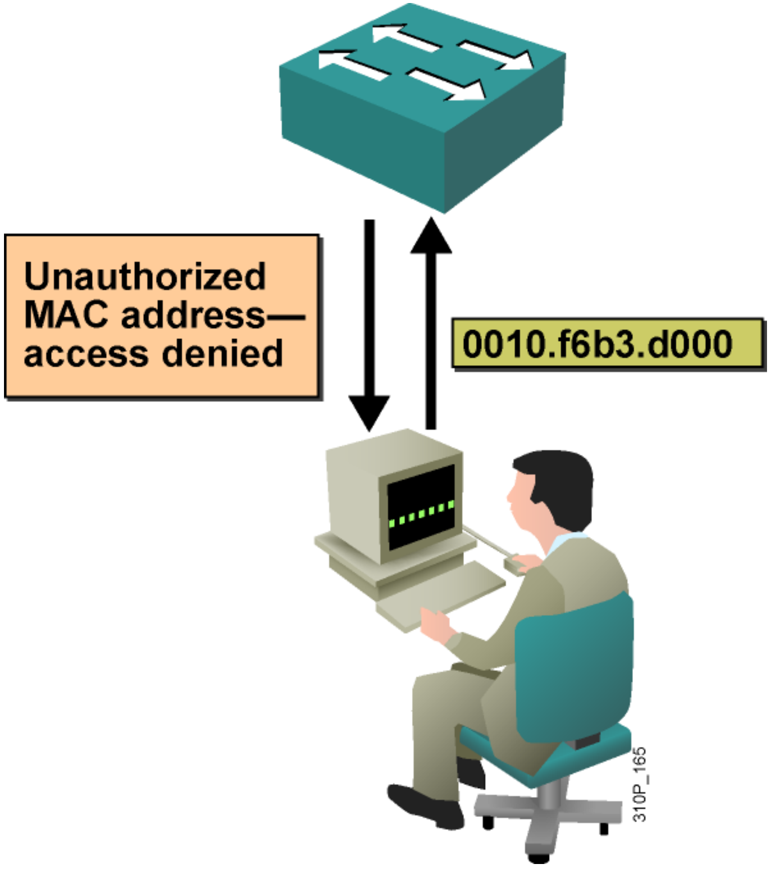
MAC Flooding

- If the attack is launched before the beginning of the day, the CAM table would be full as the majority of devices are powered on.
- Legitimate devices are unable to create CAM table entries as they power on.
- Large number of frames from a large number of devices will be high.
- If the initial, malicious flood of invalid CAM table entries is a one-time event;
  - Eventually, the switch will age out older, invalid CAM table entries
  - New, legitimate devices will be able to create an entry in the CAM
  - Traffic flooding will cease
  - Intruder may never be detected (network seems normal).

Suggested Mitigation for MAC Flood Attacks

Port Security

- Port security restricts port access by MAC address.



Configuring Port Security on a Switch

```
Switch(config-if)#switchport port-security [maximum value]
violation {protect | restrict | shutdown} mac-address mac-
address
```

- Enable port security.
- Set MAC address limit.
- Specify allowable MAC addresses.
- Define violation actions.

Port Security: Static, Dynamic, Both

- A secure port can have from 1 to 132 associated secure addresses.
- After you have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:
  - **Statically**: You can configure all secure MAC addresses by using the **`switchport port-security mac-address`** *`mac-address`* interface configuration command.
  - **Dynamically**: You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
  - **Both**: You can configure a number of addresses and allow the rest to be dynamically configured.

Port Security: Static Addresses

```
Switch(config-if)#switchport port-security mac-address
0000.0000.000a
Switch(config-if)#switchport port-security mac-address
0000.0000.000b
Switch(config-if)#switchport port-security mac-address
0000.0000.000c
```

- Restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.
- When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

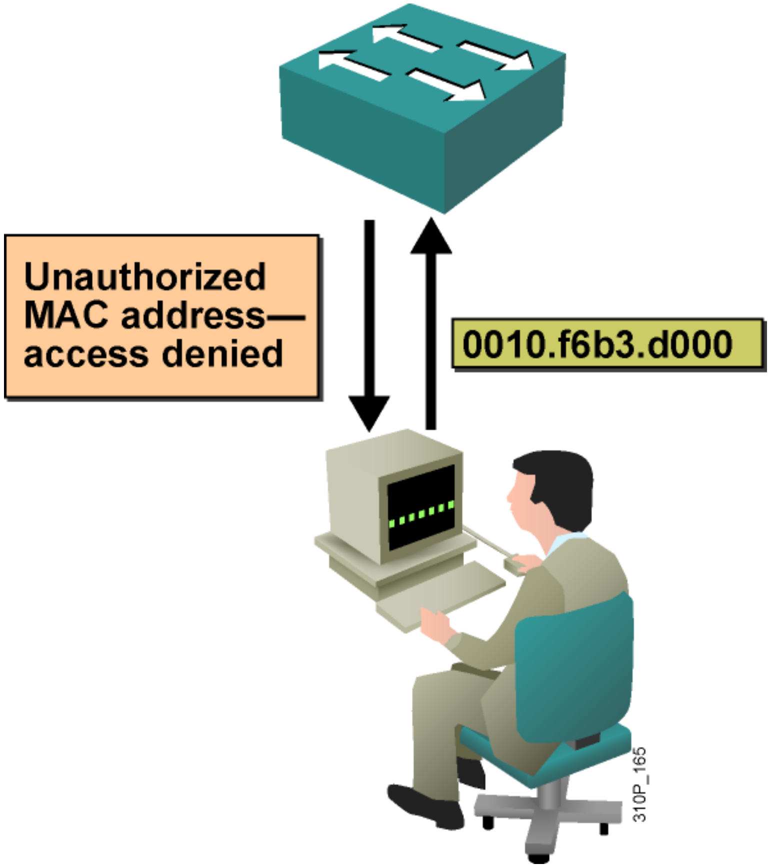
Port Security: Maximum of 1

```
Switch(config-if)#switchport port-security maximum 1
```

- The secure MAC addresses are stored in an address table.
- Setting a maximum number of addresses to **one** and configuring the MAC address of an attached device ensures that the device has the **full bandwidth of the port**.

Port Security: Violation

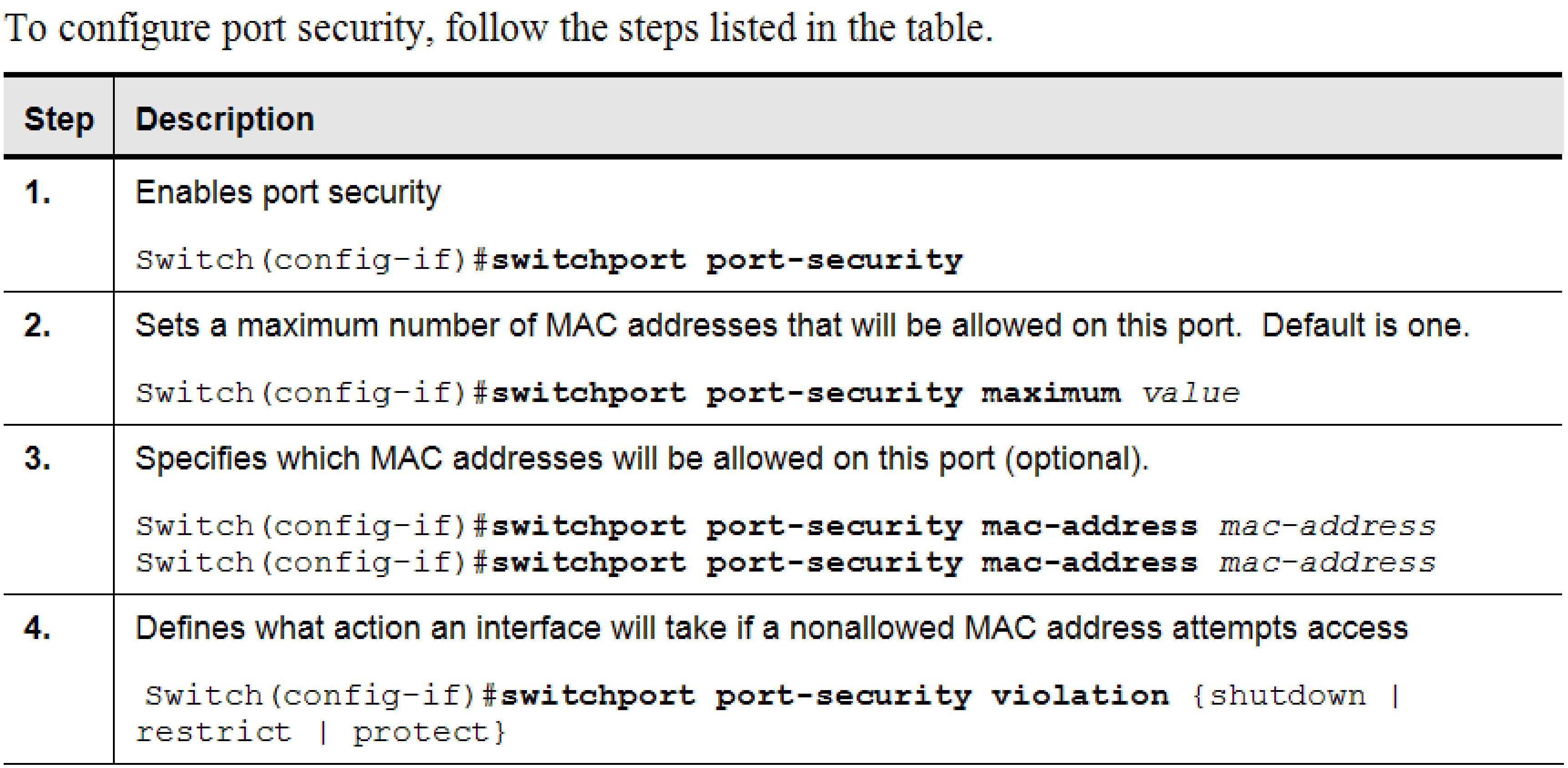
- If a port is configured as a secure port and the **maximum number of secure MAC addresses is reached**, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a **security violation occurs**.
- Also, if a station with a **secure MAC address** configured or learned on one secure port **attempts to access another secure port**, a **violation** is flagged.
- More in a moment.



Port Security: Secure MAC Addresses

- The switch supports these types of **secure MAC addresses**:
- **Static**
  - Configured using **`switchport port-security mac-address`** *`mac-address`*
  - Stored in the address table
  - Added to running configuration.
- **Dynamic**
  - These are dynamically configured
  - Stored **only** in the address table
  - Removed when the switch restarts
- ***Sticky***
  - These are dynamically configured
  - Stored in the address table
  - Added to the running configuration.
  - If running-config saved to startup-config, when the switch restarts, the interface does not need to dynamically reconfigure them.
  - **Note**: *When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. The interface adds all the sticky secure MAC addresses to the running configuration.*

Port Security: Steps



To configure port security, follow the steps listed in the table.

Step	Description
1.	Enables port security `Switch(config-if)#switchport port-security`
2.	Sets a maximum number of MAC addresses that will be allowed on this port. Default is one. `Switch(config-if)#switchport port-security maximum value`
3.	Specifies which MAC addresses will be allowed on this port (optional). `Switch(config-if)#switchport port-security mac-address mac-address` `Switch(config-if)#switchport port-security mac-address mac-address`
4.	Defines what action an interface will take if a nonallowed MAC address attempts access `Switch(config-if)#switchport port-security violation {shutdown | restrict | protect}`

```
interface FastEthernet0/2
 switchport mode access
```

- Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.

```
 switchport port-security
```

- Enables port security on the interface

```
 switchport port-security maximum 6
```

- (Optional) Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 132; the default is 1.

```
 switchport port-security aging time 5
```

- Learned addresses are not aged out by default but can be with this command. Value from 1 to 1024 in minutes.

```
 switchport port-security mac-address 0000.0000.000b
```

- (Optional) Enter a static secure MAC address for the interface, repeating the command as many times as necessary. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.

```
 switchport port-security mac-address sticky
```

- (Optional) Enable stick learning on the interface.

```
 switchport port-security violation shutdown
```

- (Optional) Set the violation mode, the action to be taken when a security violation is detected. (Next)

Port Security: Violation

```
Switch(config-if)#switchport port-security violation
{protect | restrict | shutdown}
```

- By default, if the maximum number of connections is achieved and a new MAC address attempts to access the port, the switch must take one of the following actions:
- **Protect:** Frames from the nonallowed address are **dropped**, but there is no log of the violation.
  - The *protect* argument is platform or version dependent.
- **Restrict:** Frames from the nonallowed address are **dropped**, a **log** message is created and Simple Network Management Protocol (SNMP) trap sent.
- **Shut down:** If any frames are seen from a nonallowed address, the interface is errdisabled, a **log** entry is made, SNMP trap sent and manual intervention (no shutdown) or errdisable recovery must be used to make the interface usable.

Port Security: Verify

```
Switch#show port-security
```

- Displays security information for all interfaces

```
Switch#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                   (Count)        (Count)      (Count)
---------------------------------------------------------------------------

Fa5/1                  11             11           0                Shutdown
Fa5/5                  15             5            0                Restrict
Fa5/11                 5              4            0                Protect
---------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
```

Port Security: Verify

```
Switch#show port-security interface type mod/port
```

- **Displays security information for a specific interface**

```
Switch#show port-security interface fastethernet 5/1

Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

Port Security: Verify

```
Switch#show port-security address
```

- Displays MAC address table security information

```
Switch#show port-security address
            Secure Mac Address Table
-------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
1    0001.0001.0001    SecureDynamic       Fa5/1      15 (I)
1    0001.0001.0002    SecureDynamic       Fa5/1      15 (I)
1    0001.0001.1111    SecureConfigured    Fa5/1      16 (I)
1    0001.0001.1112    SecureConfigured    Fa5/1      -
1    0001.0001.1113    SecureConfigured    Fa5/1      -
1    0005.0005.0001    SecureConfigured    Fa5/5      23
1    0005.0005.0002    SecureConfigured    Fa5/5      23
1    0005.0005.0003    SecureConfigured    Fa5/5      23
1    0011.0011.0001    SecureConfigured    Fa5/11     25 (I)
1    0011.0011.0002    SecureConfigured    Fa5/11     25 (I)
-------------------------------------------------------------------
Total Addresses in System: 10
Max Addresses limit in System: 128
```

Switch Security Issues

An Introduction

Cabrillo College

CIS 83 (CCNA 3)

Fall 2006

Rick Graziani

Fall 2006